

УДК 511.9

# ПРИЛОЖЕНИЕ БЛОЧНОГО МЕТОДА КОРКИНА–ЗОЛОТАРЕВА В МІМО—ДЕКОДИРОВАНИИ

В. С. Усатюк

E-mail: L@Lcrypto.com

В работе была показана возможность применения блочного метода Коркина-Золотарева с целью улучшения области принятия решения при декодировании сигналов в МІМО-канале. Получена верхняя оценка точности декодирования по сравнению с методом максимального правдоподобия, в случае приведения базиса блочным методом Коркина-Золотарева, при детектировании сигнала методом последовательного подавления помех.

**Ключевые слова:** решетки, МІМО, блочный метод Коркина-Золотарева.

Пусть у нас имеется МІМО-система передачи, состоящая из  $n$ — передающих и  $m$ — принимающих антенн, которая осуществляет передачу  $n$ —  $q$ — ичных символов,  $x \in C^n$ . Модель работы такой системы описывается уравнением:

$$y = Bx + \varepsilon,$$

где  $y$ —сигнал полученный приемником  $B \in C^{n \times m}$ ,  $\varepsilon$ — гауссовый шум.

Детектирование исходного сигнала в МІМО методом максимального правдоподобия (ML) эквивалентно решению уравнения:

$$x_{ML} = \arg \min_{x \in W} \|y - Bx\|^2,$$

где  $W$ — множество кодовых слов.

В силу экспоненциальной сложности метода ML— детектирования на практике применяются другие алгоритмы: обнуления (ZF), минимального среднеквадратичного отклонения (MMSE), последовательного подавления помех (SIC), см. [1].

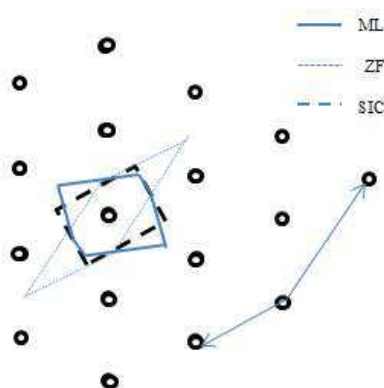


Рис. 1. Области принятия решения алгоритмами детектирования для приведенного базиса двухмерной решетки

Применение предварительного приведения канальной матрицы методами геометрии чисел позволяет получить хорошо обусловленную матрицу, тем самым улучшая область принятия решения (рис. 1), что в сочетании с вышеозначенными методами детектирования приводит к значительному энергетическому выигрышу, см. [2].

В работе [3], были получены верхние оценки для детектирования обнулением и последовательным подавлением помех в сочетании с алгоритмами приведения канальной матрицы по Ленстра-Ленстра-Ловасу [4] и Коркину-Золотареву [5]. Обобщим полученные оценки, в случае применения детектирования последовательным подавлением помех, используя блочный метод Коркина-Золотарева, см. [6].

**Теорема 1.** Пусть канальная матрица  $B$  приведена блочным методом Коркина-Золотарева, с размером блока  $2 \leq \beta \leq m$ , тогда, в случае детектирования сигнала методом последовательного подавления помех, точность декодирования по сравнению с методом максимального правдоподобия не превосходит величину:

$$\rho_{SIC} = \gamma_{\beta}^{\frac{4^{m-1}}{\beta-1}} \frac{m+3}{4},$$

где  $\gamma_{\beta}$ — константа Эрмита,  $m$ — ранг решетки.

### *Доказательство.*

По определению, точность декодирования по сравнению с методом максимального правдоподобия в случае предварительного приведения базиса и детектирования методом последовательного подавления помех, см. [3]:

$$\rho_{i,SIC} = \sup_{B_{reduced}} \frac{\lambda^2(L)}{\|b_i^{\perp}\|^2}, \quad (1)$$

где  $\lambda^2(L)$ -длина кратчайшего вектора в решетке,  $\|b_i^{\perp}\|^2$ — Евклидова норма ортогональных векторов в приведенном по Коркину-Золотареву базисе.

В работе [6] были получены оценки для базиса решеток приведенного по Коркину-Золотареву:

$$\|b_i\|^2 \lambda_i(L)^{-2} \leq \gamma_{\beta}^{\frac{2^{m-1}}{\beta-1} \frac{i+3}{4}}, \|b_i^{\perp}\|^2 \lambda_i(L)^{-2} \geq \gamma_{\beta}^{-2 \frac{i-1}{\beta-1}}, \text{ при } i = 1, 2, \dots, m,$$

где  $\lambda_i(L)$ -  $i$ -соответствующий минимум в решетке  $L$ ,  $\|b_i\|^2$ — Евклидова норма векторов в приведенном по Коркину-Золотареву базисе.

Поделив неравенства, получим  $\|b_i\|^2 \leq \gamma_{\beta}^{\frac{2^{m+i-2}}{\beta-1} \frac{i+3}{4}} \|b_i^{\perp}\|^2$ . Подставив полученное неравенство в (1), получим:

$$\rho_{i,SIC} = \sup_{B_{reduced}} \frac{\lambda^2(L)}{\|b_i^{\perp}\|^2} \leq \gamma_{\beta}^{\frac{2^{m+i-2}}{\beta-1} \frac{i+3}{4}} \|b_i^{\perp}\|^2 \sup_{B_{reduced}} \frac{\lambda^2(L)}{\|b_i\|^2}.$$

Из тривиальных соображений  $\|b_i^{\perp}\|^2 \geq \lambda^2(L)$ . Откуда получим искомую оценку:

$$\rho_{SIC} \leq \gamma_{\beta}^{\frac{4^{m-1}}{\beta-1}} \frac{m+3}{4}.$$

■

## ЛИТЕРАТУРА

1. *Yong S. C., Jaekwon K., Won Y. Y. and etc* Wireless Communications with Matlab. 2010 Wiley-IEEE Press, 544 p.
2. *Wubber D. C., Seethaler J., Matz G.* Lattice reduction // Signal Processing Magazine. IEEE. 2011. V. 28. № 3. pp. 70–91.
3. *Cong L.* On the Proximity Factors of Lattice Reduction-Aided decoding. // Signal Processing, IEEE Transactions on. 2011. V. 59. № 6. pp. 2795–2808.
4. *Lenstra A. C., Lenstra H., Lovasz L.* Factoring polynomials with rational coefficients. // Math. Ann. 1982. V. 261. № 4. pp. 515–534.
5. *Lagarias J. C., Lenstra H. W. Jr., Schnorr C. P.* Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. // Combinatorica. 1990. V. 10. № 4. pp. 333–348.
6. *Schnorr C. P.* Block reduced lattice bases and successive minima. // Combinatorics, probability and computing. 1994. V. 3. pp. 507–522.

*Usatyuk V. S.* **APPLICATION OF LATTICE REDUCTION BLOCK KORKIN–ZOLOTAREV METHOD TO MIMO–DECODING.** This article present a application of Block Korkin–Zolotarev lattice reduction method for Lattice Reduction–Aided decoding under MIMO–channel. We give a upper bound estimate on the lattice reduced by block Korkin–Zolotarev method (BKZ) for different value of the block size and detecting by SIC.

**Keywords:** *lattices, MIMO, block Korkin–Zolotarev, BKZ.*

**Усатюк Василий Станиславович** — . E-mail: **L @Lcrypto.com**